Articolo, traduzione e ricerche a cura di Davide Santoro – davidesantoro1987@gmail.com

Breve presentazione:

Il 29 Giugno 2016, l’Istituto per gli Studi Strategici[1] ha pubblicato un volume di 113 pagine dal titolo: “NATO Cyberspace Capability: A Strategic and Operational Evolution”[2] scritto da Jeffrey L.Caton[3].

Il volume analizza la struttura della NATO ed utilizza un linguaggio molto semplice ed abbastanza schematico(particolarmente utile la tabella divisa per anni contenente i momenti salienti della strategia NATO sulla cyber policy, presente all’inizio del volume).

Inoltre, questa ricerca si rivela molto interessante ed utile per tutti coloro che vogliano approfondire la struttura della NATO ed approfondire la propria conoscenza dell’Alleanza Atlantica; potreste per esempio scoprire che il “NATO Defense College”[4], l’istituto creato per “indirizzare le questioni di cyber defence ad un livello strategico, concentrandosi sulle relative implicazioni geopolitiche” si trovi a Roma, all’interno della città militare della Cecchignola.
E’ senza dubbio una lettura fortemente consigliata a tutti coloro che si interessino dei seguenti temi:

- Geopolitica
- Nato
- Sicurezza informatica

---

[1] http://strategicstudiesinstitute.army.mil/ - Si tratta del collegio bellico dell’esercito degli Stati Uniti, è una fonte ufficiale di informazioni e notizie – In lingua inglese
[2] http://strategicstudiesinstitute.army.mil/pubs/download.cfm?q=1321 – Link per scaricare il volume in formato .PDF – In lingua inglese
[3] http://strategicstudiesinstitute.army.mil/pubs/people.cfm?authorID=939 – Scheda di Jeffrey L. Caton sul sito dell’Istituto per gli Studi Strategici – In lingua inglese
[4] http://www.ndc.nato.int/ - Sito web ufficiale del “Nato Defense College”; il sito è disponibile in inglese ed in francese

Breve introduzione:

Lo sviluppo delle capacità di difesa del cyberspazio voluto dalla NATO ha registrato progressi costanti fin dalla sua introduzione al Vertice NATO di Praga del 2002[5]. Avendo subito numerosi attacchi informatici, come quelli avvenuti in Estonia nel 2007[6], la NATO ha formalizzato le sue priorità di cyber difesa nelle successive "policies" adottate rispettivamente nel 2008, 2011[7] e 2014[8].

Questa monografia esamina sia lo stato passato che quello attuale degli sforzi per la difesa del cyberspazio all'interno della NATO con l'obiettivo di valutarne l'adeguatezza nell'affrontare le minacce per i paesi membri, compresi gli Stati Uniti.

L'analisi si concentra soprattutto sulla storia recente degli sforzi NATO per la difesa del cyberspazio e di come i cambiamenti nella strategia e nella politica della NATO coinvolgano la natura emergente del cyberspazio sia per le forze militari che per altri elementi di potere.

Inizialmente il volume analizza la recente evoluzione delle fondamenta strategiche della cyber policy della NATO, della relativa governance e di come questi elementi si siano evoluti nel corso di questi 13 anni. Successivamente, delinea le principali aree di missione di cyber difesa della NATO, che comprendono la protezione del network NATO, la condivisione della conoscenza circa la situazione nel cyberspazio, la protezione delle infrastrutture critiche, la lotta al terrorismo, il supporto per sviluppare le capacità relative alla cyber difesa di un paese membro e la risposta alle crisi legate al cyberspazio.

Infine, vengono discusse diverse questioni chiave per la nuova politica avanzata di Cyber Defence che afferma come il ruolo di difesa cyber della NATO contribuisca attivamente alla missione di difesa collettiva e sostiene l'idea che un attacco cyber possa portare ad evocare le azioni previste dall'Articolo 5 dell'Alleanza[9].

Questa monografia si conclude con una sintesi dei principali risultati(ed obiettivi ndt) delle capacità della NATO nel cyberspazio ed un breve esame delle varie implicazioni per i reparti delle forze di difesa e dell'esercito in Europa. Gli argomenti trattati includono i ruoli e l'evoluzione della dottrina, la deterrenza, la formazione ed i programmi di esercizio, la cooperazione con l'industria e le implicazioni legali.

Per chi volesse approfondire consiglio la lettura del testo "National Cyber Security: Framework Manual", scaricabile in formato .PDF a questo link:

https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf - In inglese[10]

---

[5] http://www.comitatoatlantico.it/it/documenti/dichiarazione-di-praga/ Traduzione NON UFFICIALE della Dichiarazione di Praga

[6] http://www.iar-gwu.org/node/65 - Breve articolo di approfondimento dall'"Elliott School di Affari Internazionali dell'Università George Washington" – In lingua inglese

[7] http://www.nato.int/cps/en/natolive/news_75358.htm - Articolo sul sito ufficiale della NATO relativo al 2011 e disponibile in inglese, francese, russo ed ucraino

[8] http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf - Interessante articolo sulla Cyber Defence in ambito NATO – In lingua inglese

[9] http://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=it – L'articolo 5 è il cosiddetto "articolo per la difesa collettiva"; a questo link trovate il testo(in lingua italiana) del Trattato Nord Atlantico firmato a Washington il 4 Aprile 1949

[10] L'acronimo "ccdcoe" è la NATO Cooperative Cyber Defence Centre of Excellence, presente anche su Twitter: https://twitter.com/ccdcoe